PTA Cyber Security Advisory No.:109 **23-10-2020**

Name: CISCO ASA (Adaptive Security Appliance) and FTD (Firepower Threat Defense) software SSL/TLS session Denial of Service Vulnerability (CVE-2020- 3572)

Threat Classification: Denial of Service (DoS)

Affected Systems:

Cisco ASA or FTD software with SSL/TLS messages processing feature enabled. These features include, but are not limited to, the following:

- AnyConnect SSL VPN
- Clientless SSL VPN
- HTTP server used for the management interface

Summary:

This vulnerability is due to a memory leak when closing SSL/TLS connections in a specific state. An attacker could exploit this vulnerability by establishing several SSL/TLS sessions and ensuring they are closed under certain conditions. Successful exploit may allow the attacker to exhaust memory resources in the affected device, resulting in a DoS condition.

Attack Severity	HIGH
Attack Vector	Network
Privileges required	None

For more information, please find below official link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-tcp-dos-N3DMnU4T

Recommendations:

- For detailed information of the fixed releases of CISCO ASA and FTD software for the aforementioned vulnerability, please visit following official link: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-tcp-dos-N3DMnU4T#fs

- When considering software upgrades, it is recommended to consult CISCO advisories available on the Cisco Security Advisories and Alerts page for determining the exposure and complete upgrade solution.

- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.

- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.

- Whenever required, run software with minimal access rights and privileges.

- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.

- Only use licensed software and avoid download/ use of cracked and pirated software.

- Designate a PoC from your Security/ Network team (if yet not designated), for seeking assistance and reporting security issues.

- In case of any incident, please report to this office.